Caesar Cipher

تعود فكره التشفر الى الآف الاعوام عندما اعتمد يوليوس قيصر على فكره بدائيه فى تشفير رسائله الموجه لجيشه
! اذا نظرنا الى هذه فكره هذا النظام لتعجبنا من سزاجه البناء الذى قام عليه التشفير Caesar Cipher
فهى تعتمد على نقل حروف الابجديه الى ٣ اماكن فقط من نفس الابجديه
E ممثل بالحرف A حيث يصبح الحرف
عوضا عنه F هو B و الحرف
A محل الحرف B كذلك اغسطس قام باستخدام نفس الفكره ولكن بتغيير حرف واحد فقط حيث يحل الحرف

شرح فكره عمل شفره سيزر

و كما نرى يتم تحويل الحرف الى حرف آخر يليه بثلاث حروف فى الابجديه
الحروف الابجديه بدون تشفير<=== ABCDEFGHIJKLMNOPQRSTUVWXYZ
الحروف الابجديه مشفره<====== DEFGHIJKLMNOPQRSTUVWXYZABC

و قد ظل استخدام شفره سيزر حتى القرن الماضى حيث استخدمها الروس و الالمان فى اوائل التسعينيات
و نرى احيانا استخدام لهذه الشفره حتى وقتنا الحالى استخدام على نطاق محدود و شخصى

~~~~~~
~~~~~~

Vigenère cipher

فهى تعتمد فى الاصل على شفره سيزر ولكن بتكرار ٢٦ مره و اختيار مفتاح سرى فيتم عمل جدول
للحروف الابجديه مكرره ٢٦ مره و اختيار كلمه سر يتم تكرارها عده مرات مكمله لحروف الرساله

مثال :-
كلمه السر
LEMON

الرساله بدون تشفير
ATTACKATDAWN

كلمه السر مكرره

LEMONLEMONLE

الرساله مشفره

LXFOPVEFRNHR

العامود الرأسى

الناتج الاول

الناتج الثانى

العامود الافقى

الحرف E فى العامود الرأسى

الحرف L فى العامود الرأسى

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

شرح لفكره عمل شفره فيجنيريه

و يتم فك تشفير الرساله عن طريق البحث عن الحرف الموجود

العامود الأفقي L الخط الرأسى و الخانه L ايضا فنجد ان النتيجه هى الحرف A

ثانى حرف تريد فك شفرته هو X فنذهب الى الحرف E فى العامود الرأسى ثم نبحث عن الحرف X فنجد انه فى الخانه T فى العامود الافقى

~~~~~~
~~~~~~

لا إله إلا أنت سبحانك إني كنت من الظالمين

(أسرة إبداع) أكاديمية الشروق